SIEVA

Evaluando la visibilidad de tu SIEM

JT RedIris - Zaragoza
15/06/2023

Nil Ortiz - Senior R&D Cybersecurity Engineer

Whoami

Nil Ortiz

Senior R&D Cybersecurity engineer

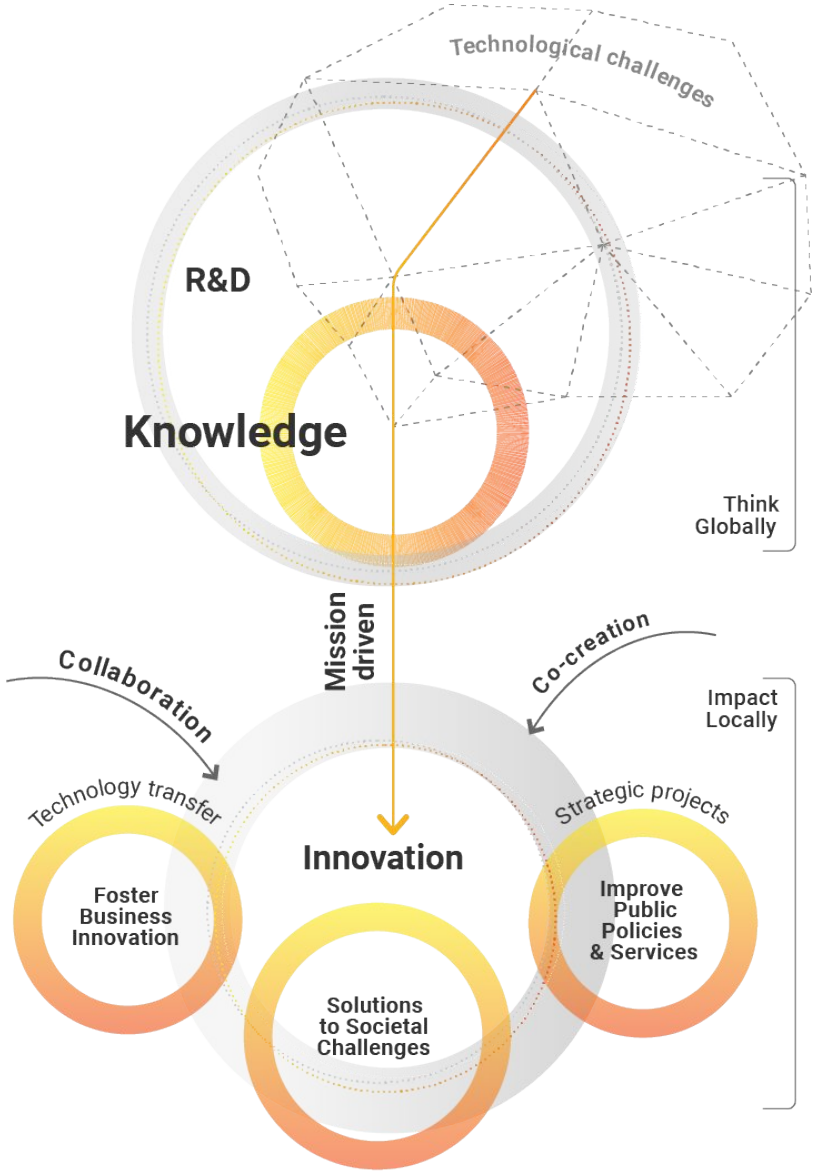
Incident response and threat intelligence analysis

Msc. in Cybersecurity

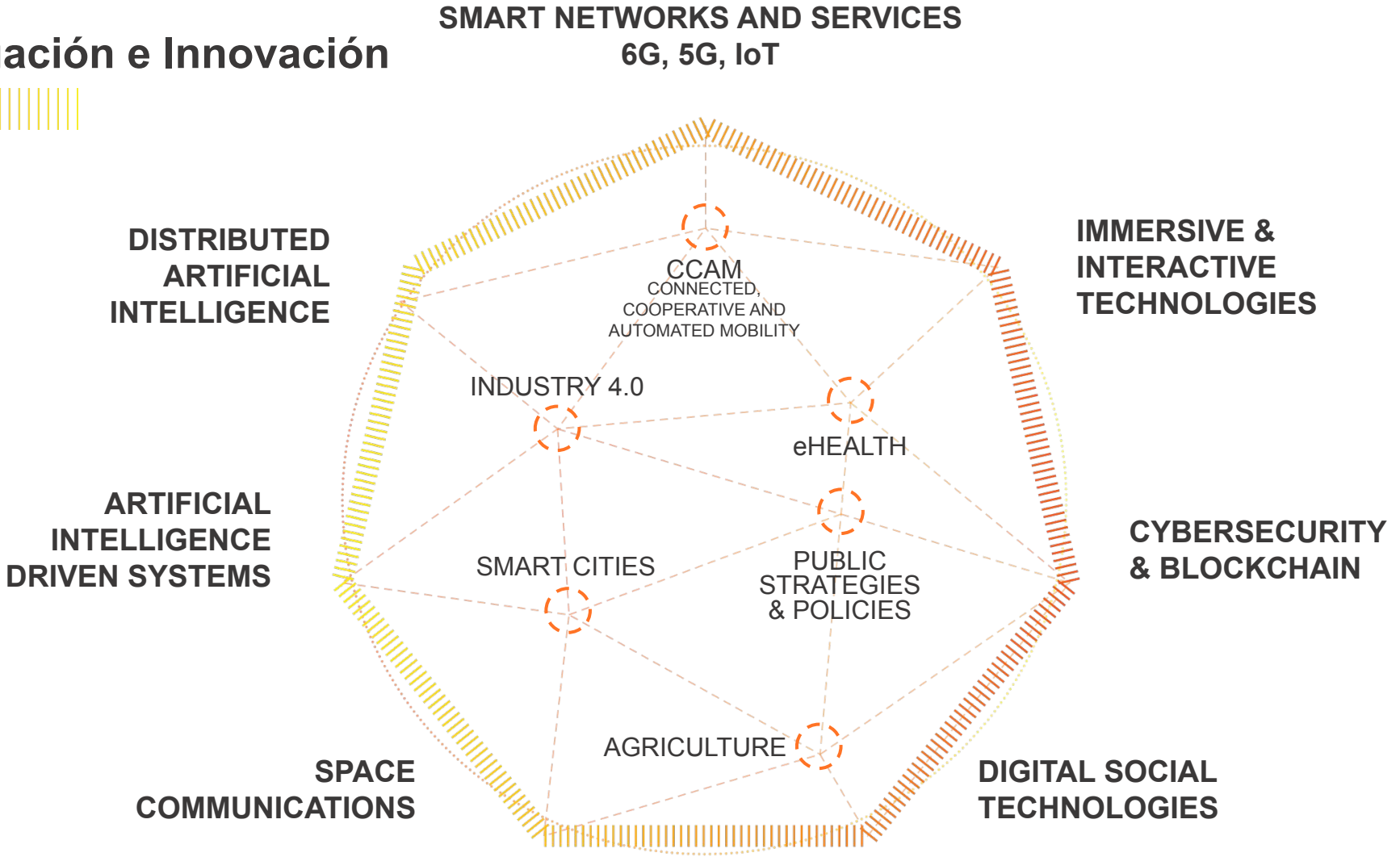
nil.ortiz@i2cat.net **LinkedIn**/in/nilortiz/

i2CAT

i2CAT es un centro de investigación centrado en proyectos impulsados por una misión para abordar el desafío de diseñar la sociedad digital del futuro basada en la investigación y la innovación en tecnologías digitales avanzadas.



Áreas de Investigación e Innovación



Iniciativas cyber + IA

DetectUEBA (Threat-Centric ML for Detection capabilities)

- Adopción de proxies de explicabilidad para la detección de amenazas
- Alinear la salida de un modelo ML con MITRE ATT&CK

openUEBA (User-Centric ML for prevention capabilities)

- Determinar patrones de comportamiento en datos históricos de usuarios
- Calcular el riesgo de una amenaza dentro de una infraestructura

SIEVA

- Evaluación de visibilidad para SIEMs
- Veamos esta herramienta en detalle …

PALANTIR
Practical Autonomous Cyberhealth for resilient SMEs & Microenterprises

ExtremeXP

TDACiberseguretat

SECANT

Innovation Programme

SIEVA

Contexto

- La mayoría de las organizaciones utilizan SIEMs como la piedra angular de sus operaciones de seguridad
- Los SIEM administran todos los datos relacionados con la seguridad y generan alertas basadas en reglas
- Para desarrollar reglas, es necesario comprender qué información se requiere de cada fuente de datos disponible

Problema

- Los SIEM son herramientas muy complejas que deben configurarse y mantenerse adecuadamente
- Los ingenieros de seguridad dedican mucho tiempo a tareas relacionadas con la ingeniería de datos.
- Las organizaciones tienen dificultades para comprender sus propias necesidades y capacidades de monitoreo

Solución

- SIEVA es una herramienta para evaluar la visibilidad de un SIEM sobre una red contra el marco MITRE ATT&CK.

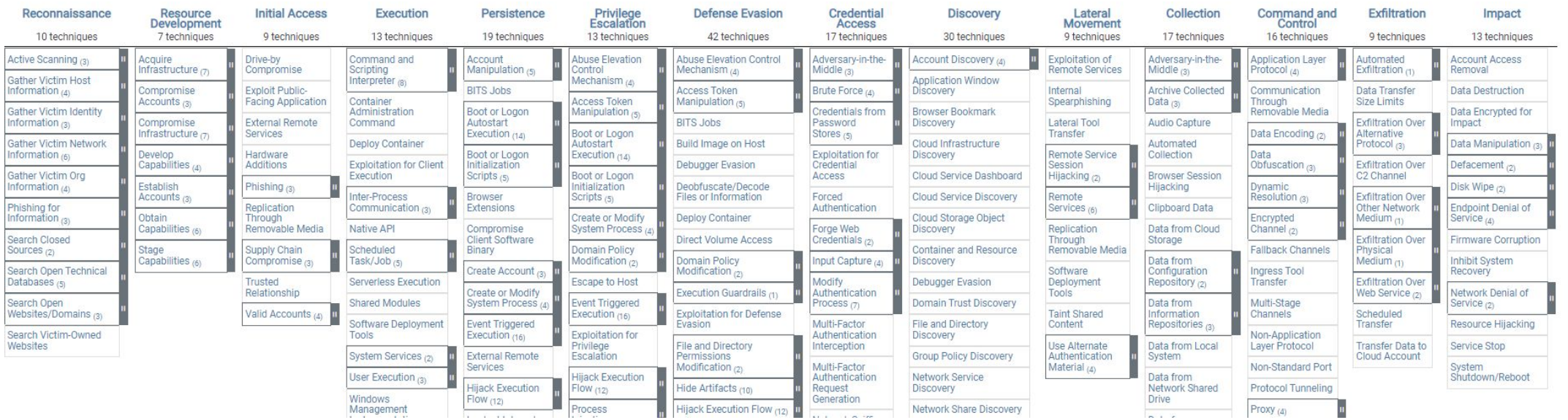
- No realiza detección, análisis, prevención, gestión de riesgos ni nada más que evaluar la visibilidad.

- Reduce la carga de trabajo de los ingenieros de seguridad que se encargan de las tareas de ingeniería de datos.

- Permite a C-suite definir mejor las estrategias a largo plazo con respecto a sus necesidades de monitoreo.

MITRE ATT&CK Framework

MITRE **ATTACK** Framework es una base de conocimiento que rastrea las **tácticas** y **técnicas** de los adversarios utilizadas por los actores maliciosos a lo largo de todo el ciclo de vida del ataque.



Arquitectura

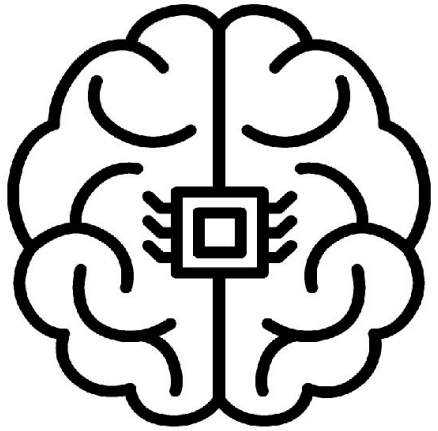
Arquitectura

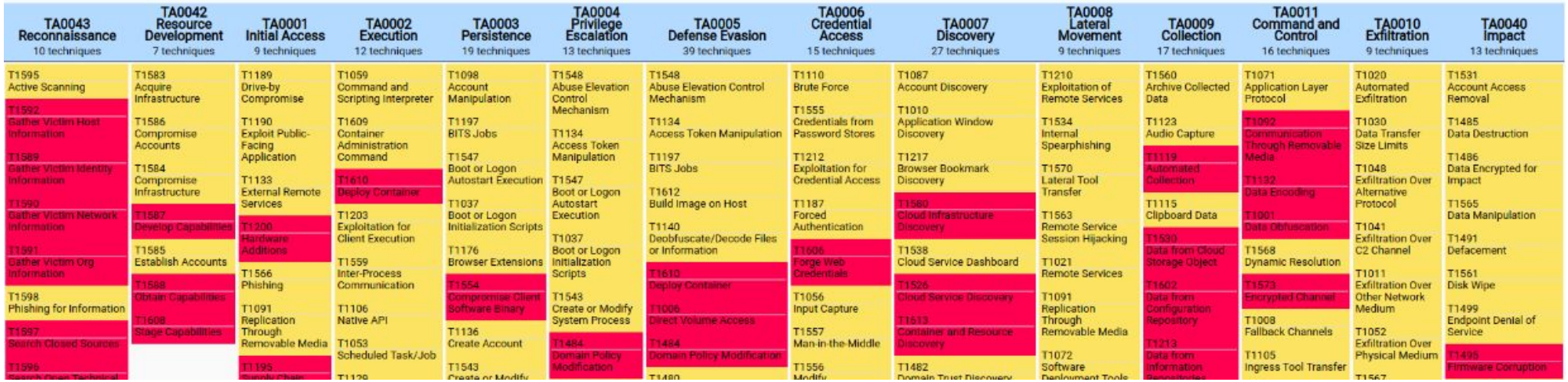
message: 1157689387.862 2 10.105.21.199 TCP_HIT/200 7256 GET http://us.i1.yimg.com/us.yimg.com/i/us/pim/dclient/d/img/md5/3c24907436896664662d0a03988cdf96_1.gif badeyek NONE/- image/gif _id: Y3rc14IBFuzzTzY2qyHi _index: webproxy-squid _score: 1 _type: _doc

message: 112.66.83.11 - - [12/Jan/2017:17:06:01 -0800] "GET /Security-Data-Analysis/Lab_1/conn.log.zip HTTP/1.1" 206 721266 "-" "Mozilla/5.0 (Linux; Android) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.131 Safari/537.36" _id: t23kPoIBFuzzTzY2R7-M _index: webserver-generic _score: 1 _type: _doc

message: Jan 20 05:59:00 198.24.1.30 dhcpd[8738]: Forward map update for 172.25.172.0 abandoned because of non-retryable failure: NXRRSET _id: V3exWIIBFuzzTzY2nJIi _index: dhcp-server-linux _score: 1 _type: _doc

message: date=2022-08-29 time=09:42:45 eventtime=1661758965179985415 tz="+0200" logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root" srcip=172.26.211.181 srcport=50595 srcintf="ssl.root" srcintfrole="undefined" dstip=172.26.211.181dstport=443 dstintf="PublicVLAN" dstintfrole="wan" srccountry="Reserved" dstcountry="United States" sessionid=33905922 proto=6 action="close" policyid=7 policytype="policy" poluuid="57d3e5c2-9c66-51eb-0af1-2582f407571e" policyname="vpn_VPNSSLPortal_toInternet" user="nil_ortiz" group="ipsec_users" service="HTTPS" trandisp="snat" transip=172.26.211.181 transport=50595 duration=1 sentbyte=3235 rcvdbyte=1831 sentpkt=9 rcvdpkt=9 appcat="unscanned" _id: Sobj6IIBFuzzTzY2X2Ij _index: firewall-fortigate _score: 1 _type: _doc





Motor IA - Como funciona?

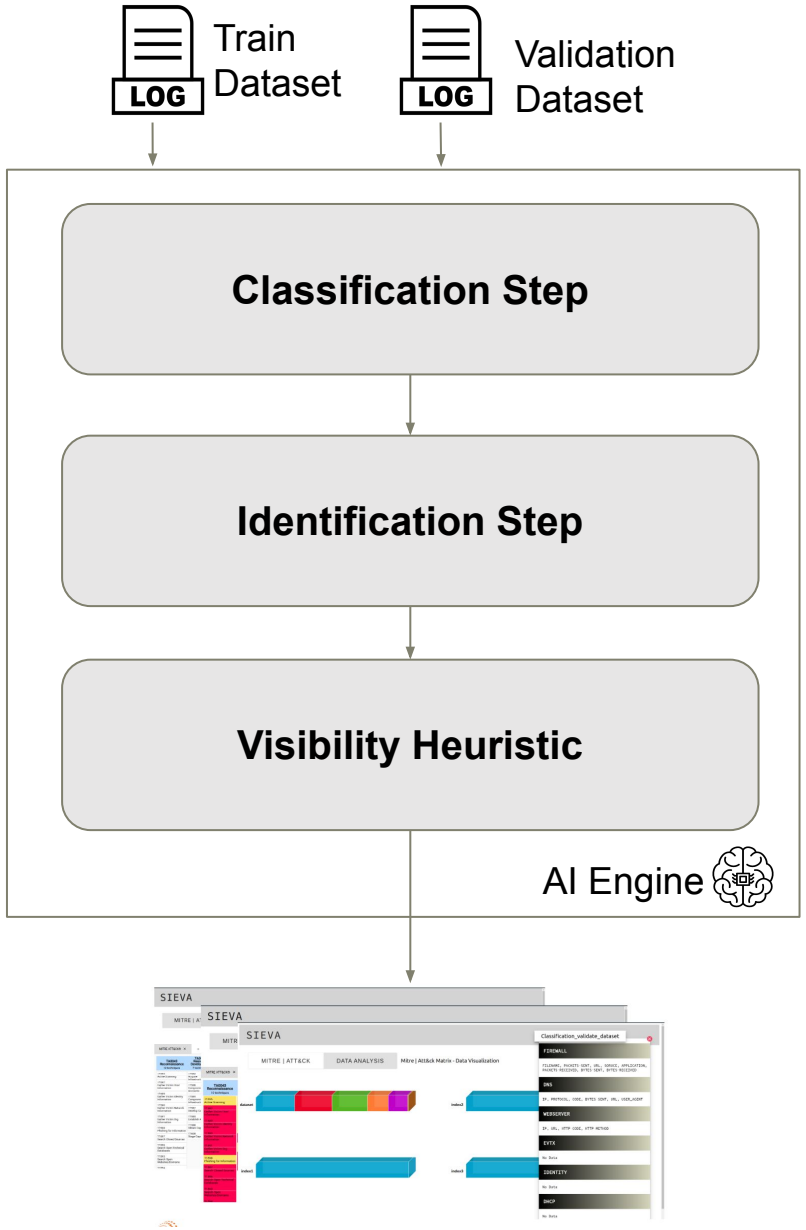
El motor de IA es un procedimiento de tres pasos:

Clasificación: Se utiliza un modelo de clasificación multiclase supervisado para determinar la tipología de registros

Identificación: Se utiliza un modelo NER personalizado para extraer entidades de los registros. *

Heurística: se utiliza la matriz ATT&CK para categorizar los registros según el grado de visibilidad

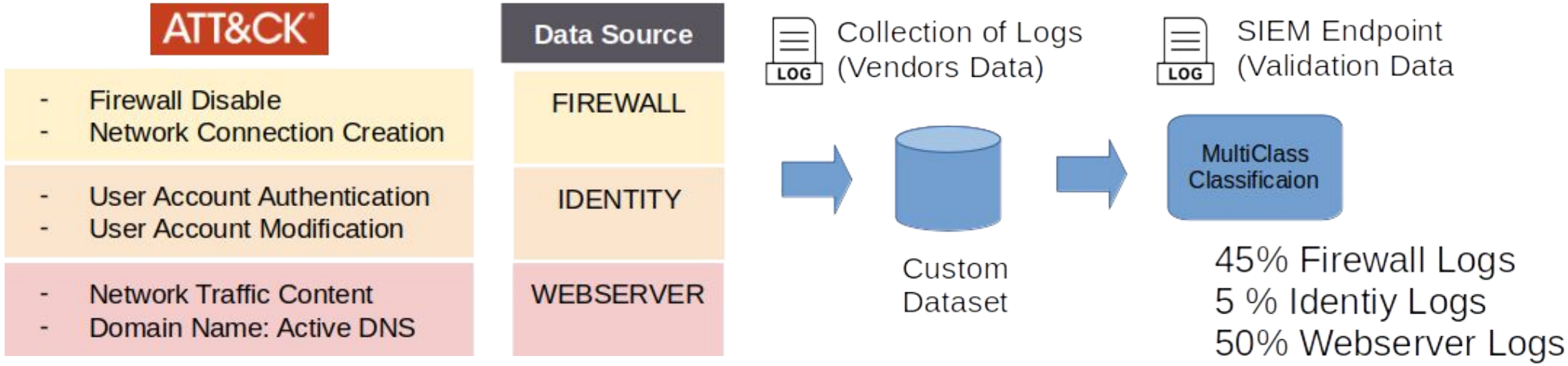
(*) Un conjunto de datos que contiene registros de diferentes proveedores, se define durante los pasos 1 y 2



Motor IA - Como funciona?

Clasificación

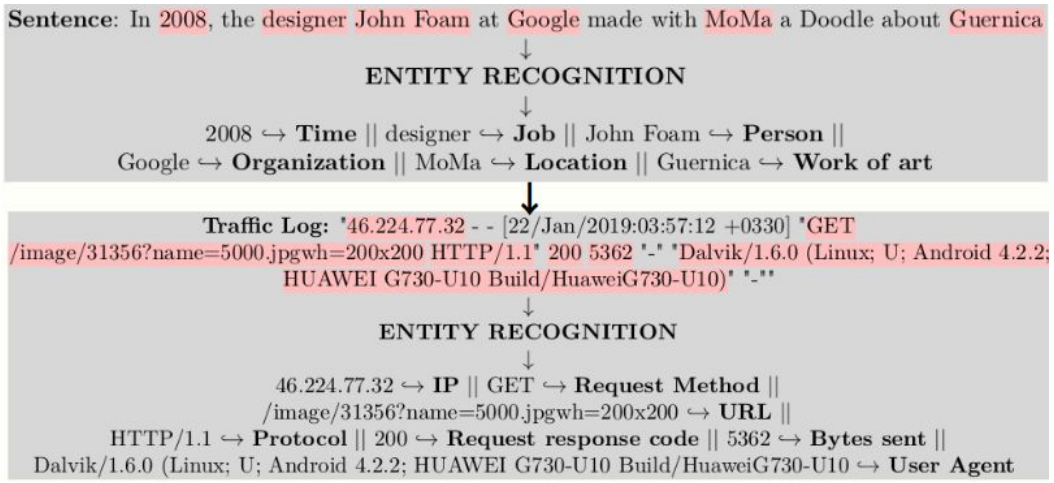
- Se utiliza un modelo de clasificación para clasificar los registros de acuerdo con las fuentes de datos definidas en MITRE ATT&CK
- Construimos manualmente un conjunto de datos utilizando muestras de registros de diferentes proveedores.



Motor IA - Como funciona?

Identificación

- Las técnicas de reconocimiento de entidades nombradas (NER) buscan localizar y clasificar las diferentes entidades en el texto en categorías predefinidas.
  - Texto plano → Registros sin procesar (RAW)
  - Categorías → IP, Dominios, host..



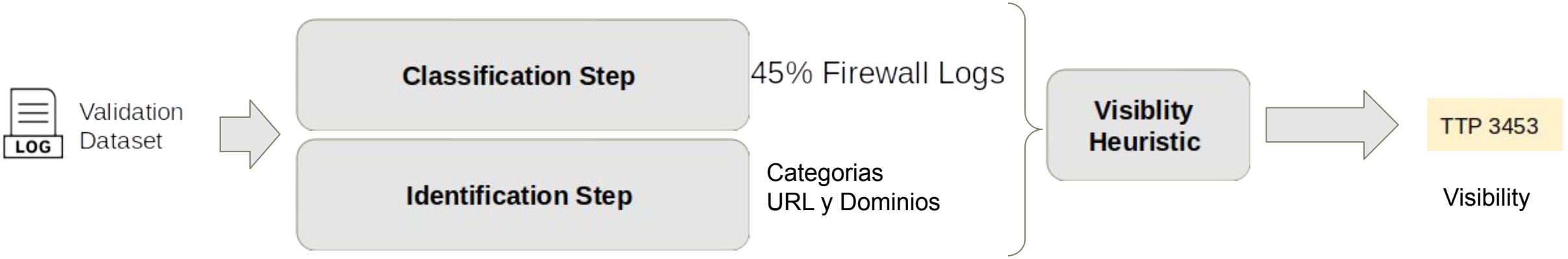
Modelo NER común

Modelo NER personalizado

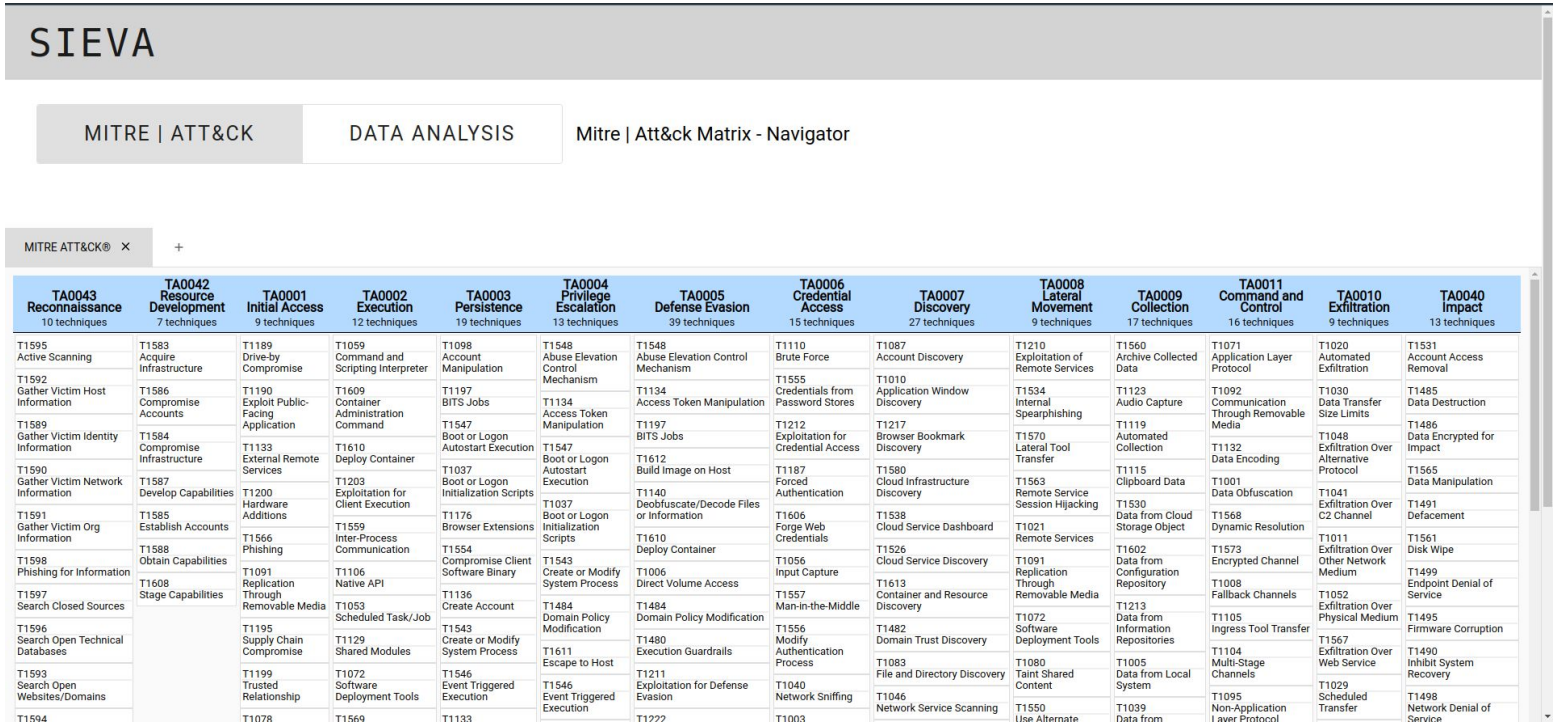
Motor IA - Como funciona?

Heurística

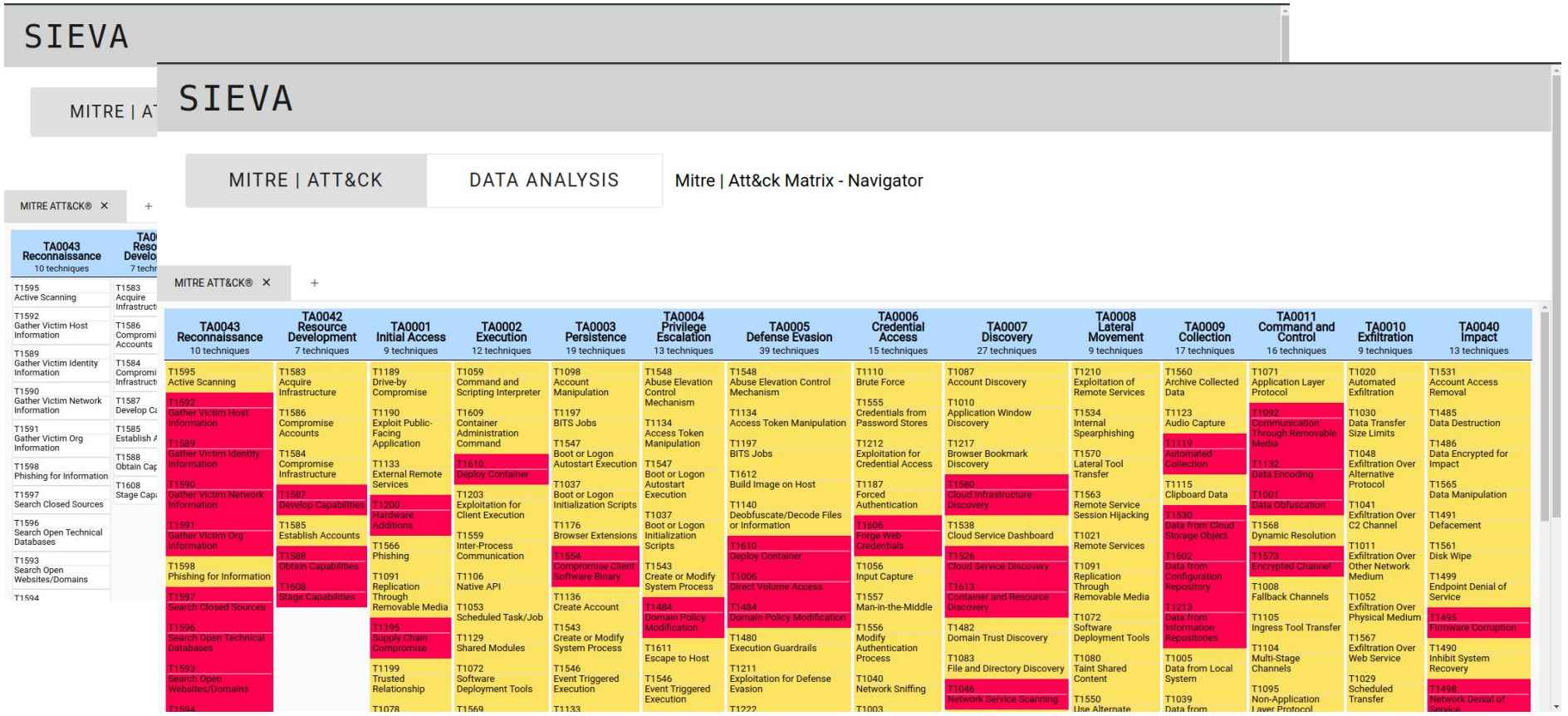
- Poner todo junto usando la representación de la matriz MITRE ATT&CK
- Se establece una heurística para asociar (Fuentes de Datos, Campos) => TTP
    - Visibilidad heurística:
        - (Sin visibilidad → 0% de precisión prevista por clase)
        - (Visibilidad parcial → !0% de precisión prevista por clase)
        - (Visibilidad → !0% de precisión prevista y > n categorías definidas)



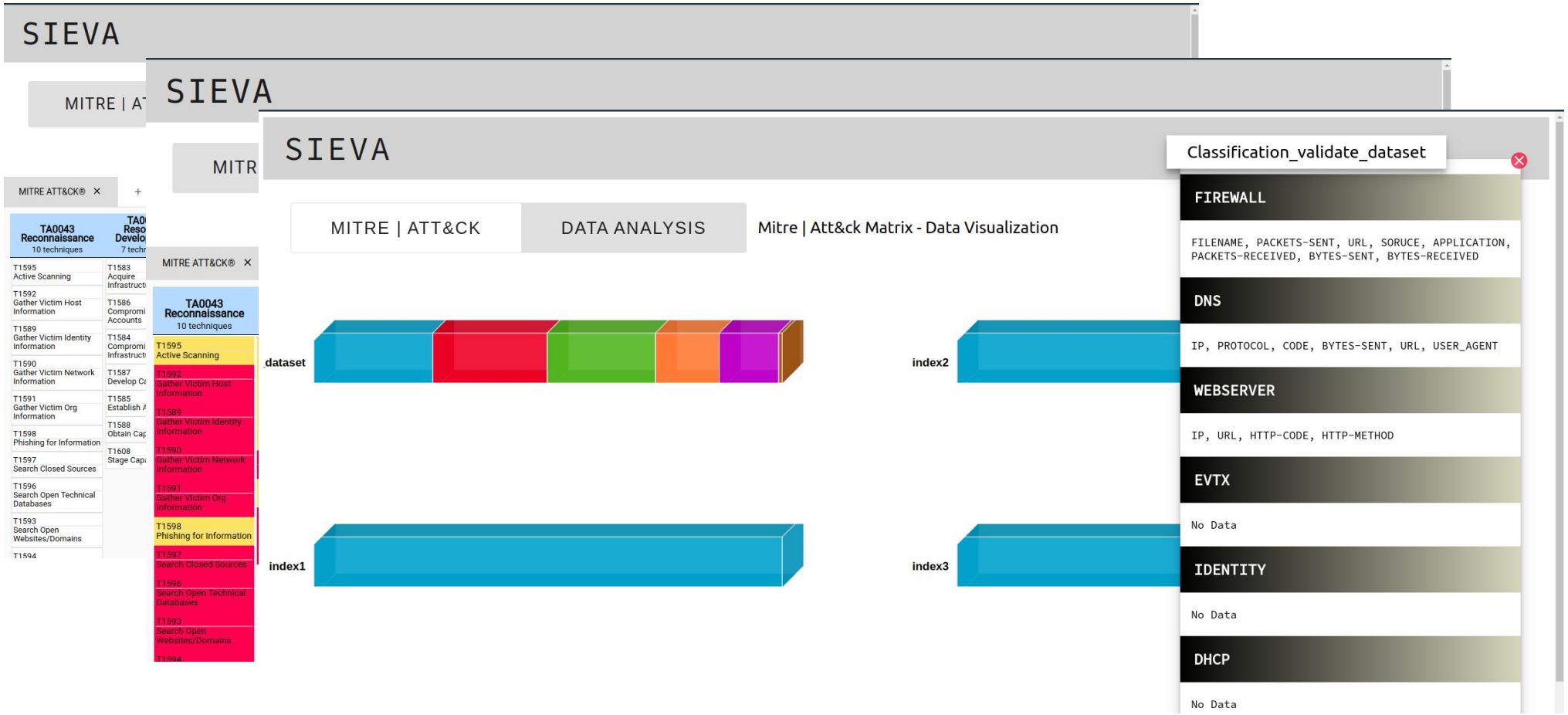
Interfaz gráfica



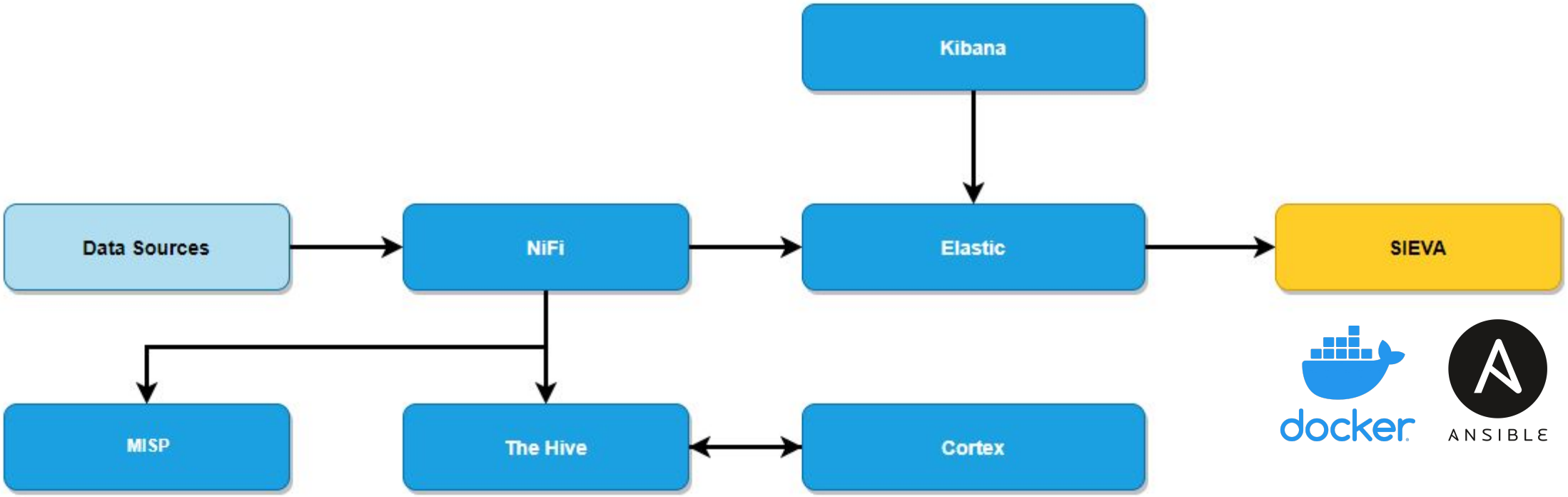
Interfaz gráfica



Interfaz gráfica



Integración en un SOC



Resumiendo

Cómo puede SIEVA ayudarte?

Reducir esfuerzos en ing. datos

Identificar lagunas en tu visibilidad

Mejorar estrategia de gestión de datos y monitorización de amenazas

SIEVA
SIEM VISIBILITY ASSESMENT

Disponible Open Source
Licencia AGPLv3

@i2CAT's Github SIEVA Repositorio
https://github.com/Fundacio-i2CAT/SIEVA

Q&A

nil.ortiz@i2cat.net

LinkedIn/in/nilortiz

Disponible Open Source
Licencia AGPLv3

@i2CAT's Github SIEVA Repositorio
https://github.com/Fundacio-i2CAT/SIEVA